Commonwealth of Massachusetts
Executive Office for Administration and Finance
Information Technology Division

Policy Area: Security	**Policy #:** ITD-01-1
Title: Enterprise Information Security Policy	**Effective Date: 11/27/01**
Applies To: All agencies within the Executive Department	**Review Date: 5/27/02**
	Revision Date:

Introduction and Scope

Information is collected, maintained and used by the Commonwealth of Massachusetts to fulfill the objectives of state government, which is to serve the people of Massachusetts. The objective of information security is protecting the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of integrity, confidentiality and availability. The information must be secured against unauthorized use or misuse, disclosure, inappropriate modification, destruction, loss, and denial of use. This policy has been written to provide basic requirements regarding the security of information maintained within electronic systems ("Information Technology" or "IT" systems). This policy governs the security of the Commonwealth's IT systems. This policy applies to all agencies within the Executive Department.[1] We recommend that the Constitutional Offices, the Judicial and Legislative branches and other governmental entities of the Commonwealth of Massachusetts adopt this or a similar policy.

Other policies address information in printed form. For guidance on securing information available on non-IT media (e.g. paper printouts), see the Records Retention Law, Mass. Gen. L. ch. 66, sec. 8; the Fair Information Practices Act, Mass. Gen. L. ch. 66A, the Freedom of Information Act (also known as the "Public Records Law"), Mass. Gen. L. ch. 66, sec. 10, the regulations promulgated under the foregoing laws, and Executive Order 412. These laws and the foregoing executive order also apply to IT information and data. Additional reference materials and guidance may also be found in the publications of the American Institute of Certified Public Accountants, the Information Systems Audit and Control Foundation/IT Governance Institute, British Standards Institution, International Organization for Standardization, National Institute of Standards and Technology and the U.S. General Accounting Office.

Terms used in this policy are defined as set forth in the section entitled "Definitions" on pages 5 to 8.

Ownership

The cornerstone to enterprise-based data security rests with enterprise data or information architecture, established ownership, rules of information ownership and custodial responsibilities, defined security requirements, established security levels, and the mechanisms to support the security levels, to meet the requirements of security. The information obtained, created, stored, provided and used must be examined to determine the necessary security. Secondly the systems and media, upon which the data resides, must be reviewed and secured to insure the integrity of the information.

[1] The Executive Department is comprised of the Executive Branch minus the Constitutional Offices, i.e., the State Auditor, State Treasurer, the Attorney General, and the Secretary of the Commonwealth.

Management has a responsibility to ensure that the organization provides all users with a secure information systems environment. To secure the information, policies governing the use and maintenance of the information must be written, accepted and adhered to. Control objectives, risks and exposures, and the position of IT governance with respect to data integrity, security, availability and ethical use shall be detailed in the security policies of the Commonwealth. The heads of secretariats, departments, agencies, colleges, and the state university system and other entities are the owners of the information within their entity and are thus responsible for the information within their purview. These individuals cannot delegate their responsibility. However they can delegate their authority and the daily tasks necessary to insure the security of their information and systems. The owners are always responsible for the information entrusted to their care.

The owners shall insure that adequate security policies are written and followed by the entity for which they are responsible. Each entity shall have policies regarding 1) information security, 2) acceptable use of the information and IT systems, both hardware and software, 3) risk analysis, data classification and business continuity, 4) physical security, 5) training of the agency's personnel, 6) copyright protection, and 7) other policies governing information and IT systems as deemed necessary. The owners shall enforce the security policies to insure the protection and integrity of the entity's information.

Management of Information and IT Systems

The Owner (or Agency Head) may assign responsibility for Agency information security to an Agency Information Security Officer ("ISO"). The Information Security Officer should have direct authority for establishing and administering the Agency's information security program. The ISO may be the agency's Chief Information Officer. However, care should be taken to ensure the proper checks and balances and segregation of duties. The person functioning as the ISO may report to the owner of the information (i.e., the head of the branch of government, secretariat, department, agency, college, or authority).

The owner's responsibilities include ensuring that appropriate internal and general controls are in place and in effect to provide reasonable assurance that control objectives related to information and system security are addressed. Those responsibilities include establishing control objectives and encompass a wide variety of security-related tasks and activities. Issues to be addressed include understanding of residual risk; assessment of security risks, objectives and controls; monitoring and evaluation; and assurance mechanisms.

The identification of where the information resides should be augmented by identifying system interfaces for information sources and destinations, as security controls would need to be applied to both. The identification of the information should lead toward defining the enterprise's data or information architecture model. This, in turn, leads one to establishing data syntax rules, corporate data dictionary, and data classification schemes. The identification of the information serves as a primary foundation upon which the organization establishes, implements and exercises security controls appropriate to the classification scheme. The objectives of information security are the integrity, confidentiality and availability of the information. To accede with their responsibilities, the owners of the information must insure that adequate security is maintained over the information and the systems, which process and maintain the information.

Acceptable Use

The owner of the information is responsible to insure that the use of information and IT resources is in conformance with stated policy and are used solely for intended, authorized purposes. Many agencies must restrict the access to, and use of, their information because of federal law, state privacy law, and separation of powers within the branches of government. Such restrictions may not result in the total isolation of agencies from participation in the larger IT environment of

the Commonwealth. Inter-agency access should be adequately addressed in policy and the Information Technology environment's design.

By applying the mechanisms of organizational, logical access security, and physical security we guard against unauthorized access that, in turn, could lead to unauthorized use, alteration, disclosure, or loss of information. In addition, unauthorized access could lead to contract infringement due to the failure to protect proprietary information. Unauthorized changes could lead to a loss in the integrity of information. The owner must also apply information security controls to prevent the loss of data availability by guarding against denial of service attacks and by developing appropriate contingency plans in the event of damaged or lost data files, or systems becoming inoperative or inaccessible. Owners must also have controls in place to prevent unauthorized disclosure via employees, third parties, or systems having authorized access to the data or information.

All users of information systems and IT Resources in the Commonwealth are responsible for their actions. Misuse of information and IT Resources may lead to consequences as detailed in the policies, executive orders and laws of the Commonwealth of Massachusetts and its' entities.

Owners of the information must clearly define the appropriate and inappropriate uses of information and IT resources.

- All entities must formally adopt, and comply with, an acceptable use policy. The Executive Office of Administration and Finance (EOAF) has issued an Acceptable Use Policy (AUP) that contains minimum requirements. The AUP is available on the Internet at http://www.state.ma.us/eoaf/anf-aup.htm. Entities may use the EOAF policy or augment it with additional procedures and guidelines for the use of IT resources within their organizations.
- Entities must provide a copy of the entities' acceptable use policy to each new and current employee and ensure that it is enforced.
- Entities must insure that temporary employees and third parties adhere to Paragraph Six of the standard terms and conditions contained in the Commonwealth's standard contract, which requires that they maintain the confidentiality of the information obtained by them in the course of their work with the Commonwealth.
- Entities may consult Executive Order 286 in the development and enforcement of policy regarding the use of software. The Commonwealth and its users must not commit copyright infringement.
- Entities must examine the activities of employees, third parties, users and anyone with access to the information and IT systems to insure that these policies are being followed.

Inventory and Classification

Classification of information is the process of establishing which information assets are to be protected to a specified level of effort and cost. To implement comprehensive security controls, owners must inventory and classify their information. The systems, which process and maintain the information, must also be classified. A system may include the information, and the supporting hardware, software, and network infrastructure used to access, manipulate, transport, and store it.

- Owners (e.g., Agency heads) should ensure that each system and the information within it, is analyzed and classified in order to determine its value and importance to the organization. The owner may consider the rating scales used by other entities including the National

Institute of Standards and Technology's Federal Information Technology Security Assessment Framework.

- At a minimum, the analysis of information systems must include consideration of the integrity, confidentiality and availability of the system and information. Classification includes the determination of the amount of time the information and system can be unavailable. Owners should know and have documented the costs and ramifications of a temporary or permanent loss of information and/or systems. Business continuity in the event of a disaster must be documented.
- The owner should have a business contingency plan developed and documented including plans to recover the information and IT system in the event of loss.

General and other Controls

The Entity's Information Security Policy should contain sections pertaining to controls, their implementation and monitoring. These policies must address controls over information as it travels through the Commonwealth's environments. For example, networks require a wide range of security controls. Information systems and information are particularly vulnerable to unauthorized access and/or alteration during transmission. The Entity's Information Security Policy should also address these controls:

- Networks must provide end-to-end security appropriate to the nature of the data that is being transported.
- Commonwealth staff access to internal networks must be subject to access control procedures (such as identification codes and passwords).
- Remote access to an internal state network(s), including MAGNet, via the Internet or dedicated circuit connecting other external networks, must be consistent with Commonwealth remote access policy and guidelines.

Identification of users must also be addressed. Various methods of identification and authentication are available for use. Depending on the sensitivity of the environment, information and/or IT Resources, various levels of user identification may be required.

Additional controls which must be addressed include security monitoring and evaluation, assurance mechanisms, policy enforcement, personnel screening, vendor screening, audit trails, incident workflow and security breaches. Physical access and environmental controls related to IT systems and hardware facilities must have established policies and procedures to provide appropriate protection. Facilities housing information systems must be physically secured in a manner appropriate to the confidential nature of the data and the asset value of the systems. Due to the wide distribution of resources, physical security is more of a concern. On-site and off-site backup of media must also be addressed. The implemented controls must be monitored and evaluated periodically.

Risk Assessment

Agencies should quantify risk by considering the potential threats to the information, the IT system and the IT resource, and the likelihood of each threat occurring. Potential threats include the loss of the information or systems due to accident or malicious intent, loss of availability such as the system being unavailable for a period of time, and unknown changes to the information or system so the information is no longer reliable. These risks should be weighed against the value of the system by evaluating the ensuing cost if each threat were to actually occur. Costs should be interpreted broadly to include money, resources, time, and loss of reputation among others. The owner should understand the theories of "reasonable assurance", "residual risk", and the objectives of risk assessment. Security solutions should be selected based on the level of risk assessed for each information system.

Training

Training and awareness are essential components of a well-designed and executed Information Security Policy. This is the most effective means of reducing vulnerability to error and fraud, and must be continually emphasized and reinforced. Agency Information Security Policies must include a formal security-training plan that will promote awareness of the Agency's security policies and procedures.

Summary

In summary, each owner is responsible for developing information security policies and procedures for their entity. Each owner is responsible to accomplish the following within their area:

- Provide all users with a secure information systems environment,
- Secure the information, including the IT systems, within their area,
- Ensure that proper internal and general controls are in place,
- Adopt, and comply to, an acceptable use policy,
- Adopt, and comply with, policies regarding information security, data classification and risk analysis, business continuity, physical security, training, and copyright protection,
- Enforce Paragraph Six of the Commonwealth's standard contract,
- Examine the activities of their employees, third parties, users and anyone with access to their information, relating to acceptable use and confidentiality of information,
- Inventory and classify their information,
- Determine the various levels of risk to their entity's data and systems,
- Develop and implement a business continuity plan,
- Train their employees and users, and
- Conform to minimum levels of security, as stated within the policies governing the WAN, prior to initial, and continued, access to the Commonwealth's Wide Area Network.

Definitions
For purposes of this policy, the following terms are defined:

Agency is a department, bureau, commission, board, office, council, or other entity in the executive department of government, which was created by the constitution or statutes of this State.

Application is a computer program designed to collect, edit, maintain, and analyze data and to report information.

Assurance Mechanisms is a system of internal controls including monitoring, evaluation, feedback, and correction activities with respect to the proper design, implementation and operation of the system of internal controls.

Authentication is the process of verifying the identity of a user attempting to access the information or attempting to use the IT assets of the Commonwealth. Any user, either within the Commonwealth's IT systems or those users attempting to gain access to the Commonwealth's information, must be identified and authenticated.

Chief Information Officer (CIO) of the agency, department, secretariat, branch of government, authority or other entity is the person who has received the delegated authority for all information technology resources within the entity. In some entities, the CIO has the day-to-day responsibilities for planning, budgeting, deploying of, maintaining, and controlling the information technology resources of the entity. The owner is the Head (e.g., commissioner, department head, Chief Justice, Governor, etc) of the entity. The CIO and the CSO may or may not be the same person.

Chief Security Officer (CSO) of the agency, department, secretariat, branch of government, authority or other entity is the person who has received the delegated authority for insuring that the information and IT systems of an entity have adequate security controls in place and functioning so that the entity is in conformance with its' security policies and is in conformance with good practice. The CIO and the CSO may or may not be the same person.

Confidential Information is information, which is restricted in its use, access to or dissemination of, which is restricted by agency policy, law, regulation or executive order.

Custodian has actual custody of the information and IT systems of an entity (e.g., Agency, Department, Secretariat, Branch of Government, college or authority), and may provide services to the entity. For example, ITD may have custody of an agency's information and IT system's application since the processing and storage of the information and application resides on the computers at ITD.

Data is sometimes considered synonymous with information. It can also be interpreted to mean the raw, individual symbols which when collected, maintained or analyzed become information.

Database is an organized store of data.

DMZ is Demilitarized Zone. DMZ within the context of this policy is defined as a network added between a protected network and an external network in order to provide a layer of security. A DMZ is sometimes referred to as a "perimeter network".

Encryption is the process of encoding electronic data that makes it unintelligible to anyone except the intended recipient. There are different levels of encryption. Stronger levels of encryption may be more costly in terms of resources and thus be used for the most sensitive information. Lower levels of encryption may be used for less sensitive information. The use of different levels of encryption should be used based on the level of sensitivity of the data to be encrypted. Decryption is the method used to convert the coded, encrypted data to understandable form.

Enterprise is a term encompassing an entire environment. Within this policy, the term Enterprise encompasses the IT environment of the Commonwealth of Massachusetts' Executive Department. A governmental entity wanting to be a part of the Wide Area Network must conform to the minimal security requirements of this policy.

Entity is an agency, department, secretariat, authority, college or other unit of the Executive Branch of the Commonwealth of Massachusetts. When the "Entity" is referred to in this policy, the Owner or head of the agency is responsible for actions of the "Entity".

Firewalls are specialized computers and programs, residing in a virtual area between an organization's network and outside networks, which are designed to check the origin and type of incoming data in order to control access, and block suspicious behavior or high-risk activity.

General Controls are controls that operate over and within an information technology facility and/or processing environment. General control areas include IT-related organization and

management, physical and system access security, environmental protection, program change control, business continuity planning, hardware and software maintenance, IT-related asset inventory control, computer operations, and IT-related contract services.

Host is a computer that mediates access to databases and/or provides other services to a computer network.

Information is a collection of pieces of data which when collected, maintained and/or analyzed becomes usable.

Information Technology Resources or IT Resources are resources, which include computers, printers and other peripherals, programs, data, local and wide area networks, and means of Internet access.

Information Security is measures, procedures, and controls that provide an acceptable degree of safety for information and IT resources, protecting them from accidental or intentional disclosure, modification, or destruction.

Information Security Officer (ISO) is the person designated by the agency head to administer the agency's information security program. The ISO is the agency's internal and external point of contact for all information security matters. The ISO and CIO may be synonymous.

Internal Controls are the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events would be prevented or detected and corrected.

Owner is the head of the entity. The owner may be commissioner, department head, chief justice, governor, etc., of the Agency, Department, Secretariat, or other entity. The owner is ultimately responsible for the information and IT systems within his/her purview. The owner must insure that the entity for which they are responsible has the security policies and procedures in place to safeguard the information and IT resources of the entity.

Password is a string of characters known to a computer system or network and to a user who must enter the password in order to gain access to information or an IT resource.

PC is an abbreviation for a personal computer. The personal computer is designed for an individual's use rather than for use as a shared resource such as a mainframe, mid-range, or server computer.

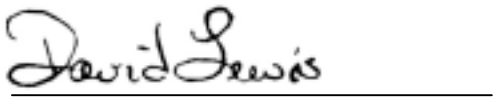
Residual Risk is risk, which is not mitigated by controls and security measures. Residual risk remains even after the proper design, implementation and exercise of a system of internal controls that provide, at least, a reasonable level of assurance that control objectives will be met. Residual risk should be identified, documented and formally accepted. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities and self-insurance.

Security Breach is an unauthorized access, loss, disclosure, modification, or destruction of information resources, whether deliberate or accidental.

Security Controls are the procedures, policies, programs, and physical safeguards including hardware, that are put in place to assure the integrity of information. Security Controls may be used to protect the means of processing information.

Sensitive Information is information that is created, received or held by agencies, which requires special precautions to protect it from unauthorized access, disclosure, modification, or deletion.

Third Party is a non-State entity that performs information technology services for, or accesses the Commonwealth's information or IT resources or, otherwise maintains a network-to-network connection with, a State agency.



November 27, 2001

David Lewis **Date**
Chief Information Officer
Commonwealth of Massachusetts

Addendum
The Enterprise Security Board is composed of thirty-two members, representing the three branches of Massachusetts's government (see below). The Enterprise Security Board provided oversight to the development of this policy beginning in May 2001. The Enterprise Security Board unanimously adopted this policy on October 24, 2001.

General Court of Massachusetts
- Senate
- House of Representatives

Massachusetts Court System
- Supreme Judicial Court
- Trial Court

Executive
- Secretary of State
- Office of the State Auditor
- Office of the State Comptroller
- Treasurer and Receiver General
- Massachusetts District Attorneys Association
- Information Technology Division
- Department of Revenue
- Department of Employment and Training
- Human Resources Division
- Operational Services Division
- Massachusetts Teachers' Retirement Board
- Division of Banks
- Executive Office of Public Safety
- Department of Mental Health
- Department of Public Health
- Department of Transitional Assistance
- Massachusetts Highway Department
- Massachusetts Office on Disability
- Department of State Police

Massachusetts Emergency Management Agency
Massachusetts Turnpike Authority
University of Massachusetts, President's Office
Bridgewater State College

The Massachusetts Water Resources Authority also attended and participated in the meeting of October 24, 2001.